Defense Information Systems Agency

A Combat Support Agency

Tactical Edge Service:
NetOps and IA Considerations

GIG EWSE IA and NetOps (EE213)
17 August 2011

UNCLASSIFIED

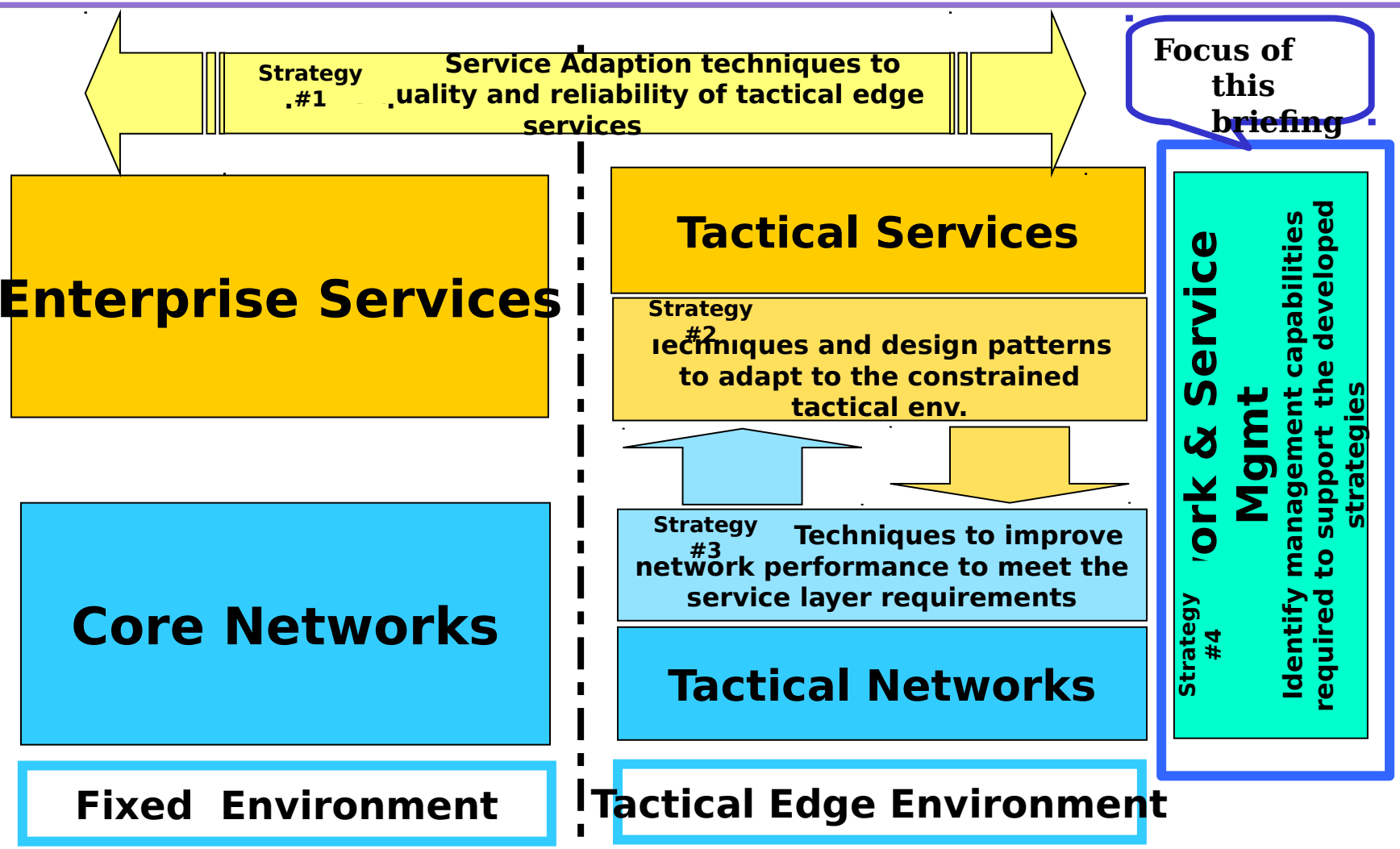
DISA
A Combat Support Agency

Agenda

- Additional Tactical NetOps Challenges
- NetOps/IA Implications of Proposed Communications and Service Delivery Solutions
- NetOps/IA Research Areas
- Summary

DISA
A Combat Support Agency

Technical Approach Framework


Strategy #1
Service Adaption techniques to uality and reliability of tactical edge services
Focus of this briefing
Enterprise Services
Tactical Services
Strategy #2
Techniques and design patterns to adapt to the constrained tactical env.
Strategy #3
Techniques to improve network performance to meet the service layer requirements
Core Networks
Tactical Networks
ork & Service Mgmt
Strategy #4
Identify management capabilities required to support the developed strategies
Fixed Environment
Tactical Edge Environment

An EWSE Approach to the Tactical Edge Service Problem

DISA
A Combat Support Agency

Why is Tactical NetOps more difficult?

- **NetOps in the fixed and tactical environments involves the same three general areas**
  - **monitoring, managing & controlling availability, allocation & performance (GEM)**
  - **protecting & defending to assure capabilities (GNA)**
  - **managing the visibility & accessibility of information (GCM)**
- **The tactical environment is made more difficult by**
  - **Operating Environment**
    - **Much more dynamic network topology**
    - **User and resource node mobility**
    - **Limited capacity, intermittent communication channels**
    - **Greater likelihood of deliberate action by adversary to disrupt/deny RF channels**
  - **Resource Limitations**
    - **Availability of trained NetOps personnel**
    - **Space, weight, and power constraints on processing, transmission & storage resources for NetOps**
    - **Availability of RF spectrum and device capabilities**
    - **Technical and procedural barriers to “resource pooling”**
  - **Organizational Structures**
    - **Need to communicate “forward”, “upward” and “laterally” among heterogeneous mix of organizational elements and systems**
    - **Complexity of operational control and reporting chains**

DISA
A Combat Support Agency

NetOps/IA Considerations for Service Adaptation Solutions

- **Tiered Service Model**
  - **“Tier” of service should be chosen based on functional requirements and network path; “best available bandwidth” rather than shortest path algorithm for service delivery point selection may be more appropriate**
  - **Need to provide mechanism for characterization of network path between end device and service delivery point**
- **Service Proxy Gateway**
  - **Asynchronous operation (e.g. store & forward) implies use of transferable user identity token/credentials or authentication of users at proxy device**
  - **Compression, data/protocol translation imply intermediate decryption/re-encryption**
  - **Cross domain invocation of services requires agreement on user identity, attributes, and authentication mechanisms**
  - **Need to consider confidentiality and integrity of stored/cached data**
  - **Intelligent content filtering requires either external tagging or visibility into payload data**
- **Service Broker**
  - **Greatest utility is when broker can access service delivery points in multiple organizations**
    - **Requires supporting policy and interoperable user identity, attributes, and authentication mechanisms**
    - **Need to monitor and manage cross-domain resource utilization**
  - **Need to verify identity of both service delivery points and users**

DISA
A Combat Support Agency

NetOps/IA Considerations for Service Design Pattern Solutions

- **Adaptive Content Delivery**
  - Needs same type of network path characterization mechanism as tiered service
- **Distributed Architecture/Runtime Binding**
  - Need to verify identity of distributed platforms
  - Need to monitor which distributed platform is being used by which user
  - May need mechanism to control distribution of load
- **Forward Caching/Store and Forward**
  - Implies use of transferable user identity token/credentials
  - Confidentiality and integrity of stored/cached data
- **Offline Mode**
  - May need to rate-limit traffic when device reconnects

DISA
A Combat Support Agency

NetOps/IA Considerations for Enhance Transport Solutions

- **Use of more sophisticated or adaptive modulation/ transmit power techniques and increased antenna gain makes RF spectrum management more complex**
- **Need agreement on QoS approach and implementation across domains; mission criticality versus transmission requirements of supported service (e.g. jitter, max latency) in packet queuing priority an open question**
- **Performance Enhancing Proxies imply intermediate decryption/re-encryption**
- **Application level gateways and security devices doing deep packet inspection need to account for payload compression**

DISA
A Combat Support Agency

Summary of NetOps/IA Considerations

- **Supporting dynamic, secure relationships between users and resources requires bi-directional endpoint authentication**
- **Sharing of resources across organizational boundaries requires both operational agreement and NetOps function to monitor and control such use**
- **Rewriting packets and/or storing information at intermediate locations requires adjustments to end to end security and key distribution model**
- **Autonomous adaptive use of physical channel resources (bandwidth/spectrum) by end devices needs to be accounted for as part of overall NetOps resource management**

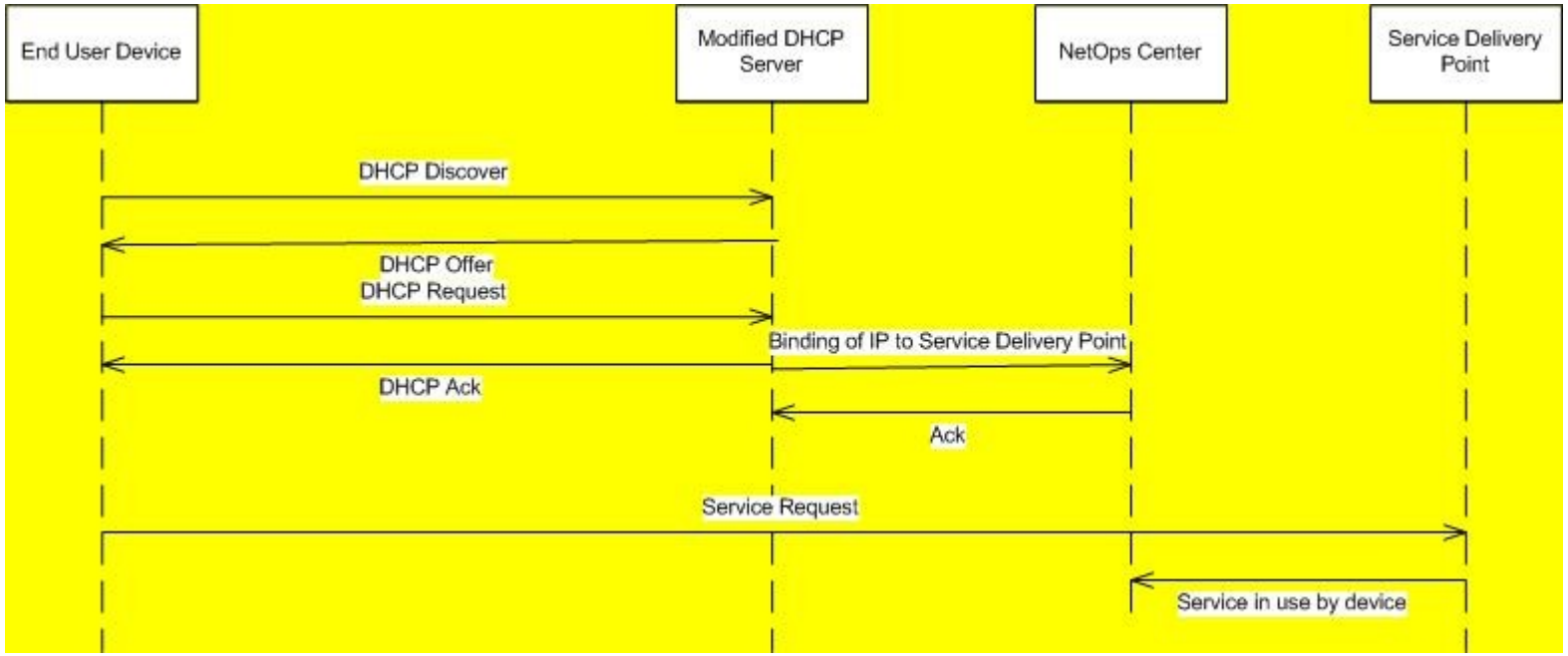
DISA
A Combat Support Agency

NetOps/IA Research Areas

- **Network Path Characterization Method**
  - potential for leveraging information exchanged as part of routing protocols
  - ongoing work in feeding link performance information into routing process
- **Interoperability of Identity and Access Control across organizational boundaries**
  - common identity solution for both users and service delivery points
  - assignment of capabilities to unanticipated users
- **Extending Service Monitoring**
  - how to identify who is utilizing a particular service
  - monitoring and controlling cross boundary service utilization
- **Spectrum Allocation and Management for Self-adaptive RF Devices**

DISA
A Combat Support Agency

Example – Use DHCP to map end devices to servers and track use



1) End device does normal DHCP discovery/request
2) Response from DHCP server includes IP addresses for end device and Service Delivery Point
3) Assignment of end device and Service Delivery Point reported to/collected by NetOps center

DISA
A Combat Support Agency

Summary

- **Issues are both technical and operational**
  - **Need agreement on sharing and management of resources on across organizations for greatest efficiency**
  - **Method for assured user identity and access control across organizational boundaries a key capability**
- **Some possible technical improvements involve straightforward extensions of existing technology**
  - **Example #1**
    - **Both Tiered Service and Adaptive Content Delivery need a network path characterization mechanism**
    - **Route computation often uses path characteristics but essentially discards this information and determines a single best route**
    - **Expand available set of route choices and associated metrics by using Neighbor Specific BGP**
  - **Example #2**
    - **DHCP in wide use to distribute client IP address, subnet mask, DNS server and gateway IP information**
    - **RFC 2132 includes option for providing multiple server addresses as part of DHCP response**
    - **Use DHCP to distribute clients among alternative servers or to service broker**

www.disa.mil